

AD736760

Economics of Reliability for Spacecraft Computers

Prepared by H. HECHT
Computer and Guidance Technology Programs

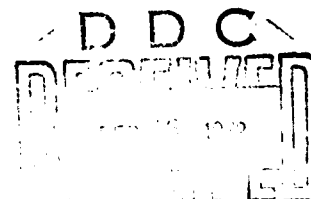
71 OCT 68

Office for Technology
THE AEROSPACE CORPORATION

Reproduced by
NATIONAL TECHNICAL
INFORMATION SERVICE
Springfield, Va 22151

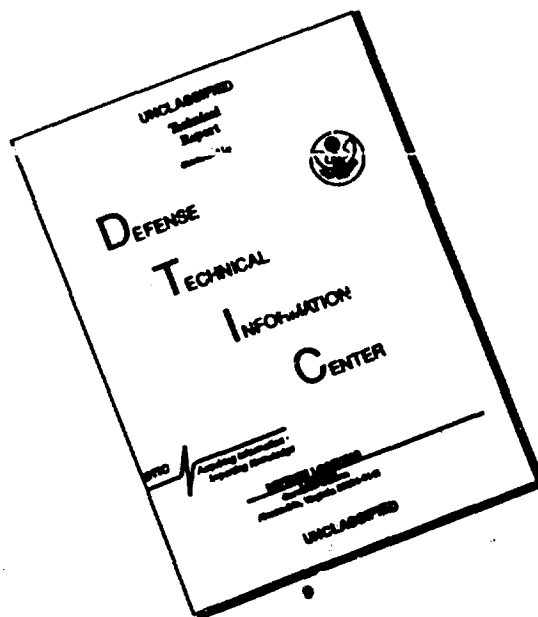
Prepared for SPACE AND MISSILE SYSTEMS ORGANIZATION
AIR FORCE SYSTEMS COMMAND
LOS ANGELES AIR FORCE STATION
Los Angeles, California

APPROVED FOR PUBLIC RELEASE:
DISTRIBUTION UNLIMITED



38

DISCLAIMER NOTICE



**THIS DOCUMENT IS BEST
QUALITY AVAILABLE. THE COPY
FURNISHED TO DTIC CONTAINED
A SIGNIFICANT NUMBER OF
PAGES WHICH DO NOT
REPRODUCE LEGIBLY.**

UNCLASSIFIED

Security Classification

DOCUMENT CONTROL DATA - R & D		
<i>(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)</i>		
1. ORIGINATING ACTIVITY (Corporate author)		2a. REPORT SECURITY CLASSIFICATION
The Aerospace Corporation El Segundo, California 90245		Unclassified
		2b. GROUP
3. REPORT TITLE		
ECONOMICS OF RELIABILITY FOR SPACECRAFT COMPUTERS		
4. DESCRIPTIVE NOTES (Type of report and inclusive dates)		
5. AUTHOR(S) (First name, middle initial, last name)		
Herbert H. Hecht		
6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
71 October 08	37	7
8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)	
F04701-71-C-0172	TR-0172(2315)-1	
b. PROJECT NO.		
c.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)	
d.	SAMSO TR-71-327	
10. DISTRIBUTION STATEMENT		
Approved for public release; distribution unlimited		
11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY	
	Space and Missile Systems Organization Air Force Systems Command Los Angeles, California	
13. ABSTRACT		
<p>To achieve an economically optimum level of reliability each improvement step is warranted only if the expected reduction in cost of failure exceeds the cost of the improvement. To this end, techniques for calculating cost of failure are described, in particular a new technique for evaluating cost of failure for long-time spacecraft missions. Guidelines for assessment of the economic impact of various improvement techniques are presented.</p>		

UNCLASSIFIED

Security Classification

14

KEY WORDS

Reliability
Economics of Reliability
Cost of Reliability
Cost of Failure
Spacecraft Computers
Spacecraft Systems
Computers
Cost Models
Mission Analysis
Long-Life Missions

Distribution Statement (Continued)

Abstract (Continued)

Unclassified

Security Classification

Air Force Report No.
SAMSO TR-71-327

Aerospace Report No.
TR-0172(2315)-1

ECONOMICS OF RELIABILITY FOR
SPACECRAFT COMPUTERS

Prepared by
H. Hecht
Computer and Guidance Technology Programs

71 OCT 08

Office for Technology "
THE AEROSPACE CORPORATION
El Segundo, California

Prepared for
SPACE AND MISSILE SYSTEMS ORGANIZATION
AIR FORCE SYSTEMS COMMAND
LOS ANGELES AIR FORCE STATION
Los Angeles, California

Approved for Public Release;
Distribution Unlimited.

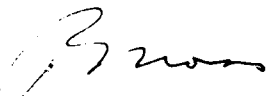
FOREWORD

This report is published by the The Aerospace Corporation, El Segundo, California, under Air Force Contract F04701-71-C-0172.

The author wishes to acknowledge the contributions of H. D. Wishner, Computer and Digital Subsystems Department, in the development of the time-dependent cost of failure model.

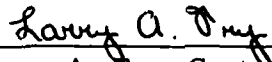
This report, which documents research carried out from April 1971 through September 1971, was submitted

Approved



B. Moss, Director
Technology Programs
Office for Technology

Publication of this report does not constitute Air Force approval of the report's findings or conclusions. It is published only for the exchange and stimulation of ideas.



Larry A. Fry, Capt, USAF
System Program Data Mgmt Ofcr
Computer Technology Office
Deputy for Technology

ABSTRACT

To achieve an economically optimum level of reliability each improvement step is warranted only if the expected reduction in cost of failure exceeds the cost of the improvement. To this end, techniques for calculating cost of failure are described, in particular a new technique for evaluating cost of failure for long-time spacecraft missions. Guidelines for assessment of the economic impact of various improvement techniques are presented.

TABLE OF CONTENTS

<u>Title</u>	<u>Page</u>
Nomenclature	vi
Section 1 Introduction	1
Section 2 Tradeoff Criteria	3
Section 3 Mission Reliability Model	7
Section 4 Time-Dependent Reliability Model	13
Section 5 Cost of Reliability Improvement	21
Section 6 Conclusions	28
References	29

FIGURES

		<u>Page</u>
Figure 1	Mission Reliability Optimization, Low Cost Spacecraft	10
Figure 2	Mission Reliability Optimization, High Cost Spacecraft	12
Figure 3	Expected Cost of Failure vs Computer Hazard	18
Figure 4	Reliability Optimization for Time-Dependent Case	20
Figure 5	Cost of Reliability Improvement	26

TABLES

Table 1	Normalized Expected Cost of Failure for the Time-Dependent Model	17
Table 2	Evaluation of Improvement by Massive Redundancy	24

NOMENCLATURE

$a \triangleq c/s$	normalized computer hazard
$b \triangleq Ws$	random failure factor
c	computer hazard (1/MTBF)
C	cost (always in monetary units)
C	(as subscript) pertaining to computer
$E[X]$	expected value of random variable X
F	failure probability (for mission or as a function of time, as identified in the context)
k_i	conversion factor to monetary units of the i^{th} nonmonetary resource
L	loss (in monetary units) when failure occurs
Q_i	quantity of i^{th} nonmonetary resource
R	reliability (for mission or as a function of time, as identified in the context)
s	spacecraft hazard (1/MTBF)
S	(as subscript) pertaining to spacecraft exclusive of computer
$U \triangleq V_{fC}/L$	normalized cost of failure due to computer
V	value (total resource requirement)
V_f	resource absorbed due to failure
V_r	resource requirement for reliability improvement
W	wear-out time of spacecraft

SECTION 1

INTRODUCTION

Reliability requirements for spacecraft computers may be dictated directly by mission considerations, or they may arise from economic tradeoffs. An example of the first category is furnished by manned vehicles where either the numerical reliability requirement for the computer is derived by apportionment of a top level safety and reliability goal, or where specific degradation patterns are demanded such as the "fail-operative, fail-operative, fail-safe" requirements for the Space Shuttle electronics. Economic considerations enter into evaluation of alternative configurations but not into the setting of the requirements.

The second category comprises most unmanned satellites, including navigation, meteorological, and general space exploration vehicles. Typically, these require reliability beyond that obtainable from a single computer, but for economic reasons they are not candidates for the massive redundancy approach which is at present being pursued in many manned programs. The reliability improvement of interest to this application area can frequently be obtained by emphasis on component reliability plus a combination of the following techniques:

- a. Coding, diagnostic programs, and reasonableness checks or duplicated computation for fault identification and location. Even ground intervention in this process is permissible in some cases.
- b. Selective redundancy of modules within a computer based on criteria of failure probability and resource requirements for each module. This is particularly effective if the basic computer employs a number of hardware-identical modules, permitting redundancy for multiple elements.
- c. Reconfiguration capability for switching in spares or optimizing the remaining computing resources after a failure.
- d. Program and system restart capability to permit resumption of operation after transient failure or after reconfiguration.

These techniques are already quite well-developed, and further improvements can be expected in the future (Ref. 1). It should be remembered that

the satellite applications addressed here are generally tolerant of short interruptions in computer availability.

To match the requirements of a specific mission with the available fault-tolerant computer technology, some economic tradeoffs must be performed, typically during early phases of program planning when very little solid reliability and cost information is available. This is the area primarily addressed here. The methodology is not completely rigorous, and the findings may be subject to various interpretations. Still, it seems desirable to propose an organized and documented approach which may guide the judgment that inevitably must be brought to bear in early phases of a program.

At present, decisions on central computer versus dedicated electronics, selection of the computer configuration and specification of the reliability requirements proceed largely intuitively. It is not claimed that the results are bad, but the procedures proposed here have advantages over the intuitive approach in at least three areas:

- a. Early identification of required data
- b. Clear rejection of undesirable configurations (even crude data usually permit this)
- c. Improved communication of tradeoff criteria among decision makers.

Properly used they improve and speed up the computer specification and selection for spacecraft in which the computer reliability is governed by economic considerations.

The tradeoff techniques used are introduced in the following section. In Sections 3 and 4, cost of failure calculations are carried out for the case of mission reliability and time-dependent reliability, respectively. Procedures for evaluating the cost of reliability improvements are discussed in Section 5, and conclusions are presented in the final section.

SECTION 2

TRADEOFF CRITERIA

The overall aim of economically motivated reliability improvement is to identify those improvements which will pay their way, i.e., those for which the cost of improvement is less than the expected cost of failure. The term "cost" denotes, in this connection, a very general sum of resources that will be either expended for reliability improvement or will be absorbed in cost of failure. As an example of resources required for reliability improvement in spacecraft computers we will be particularly concerned with equipment cost, weight, and power requirements. At times software changes, environmental protection, and input/output restrictions may also need to be considered. Specific examples in the evaluation of cost of reliability improvement are discussed in Section 5.

The expected cost of failure is evaluated by techniques covered in the following sections which take the form of the probability of a loss multiplied by the cost assigned to that loss when it does occur. This latter factor--the loss--typically includes costs of a replacement launch plus charges for unavailability of satellite services until replacement is accomplished, for failure investigations, and for side effects.

Both the cost of reliability improvement and cost of failure involve some terms which are normally expressed in monetary units and some that are not. For the latter it is assumed that suitable dollar tradeoffs can be established, although it is realized that difficulties and uncertainties will be encountered in this area. We may find it convenient to designate the general resource (for cost of improvement or of failure) as V which we associate with the term "value". This resource will consist of one or more direct monetary costs plus a number of nonmonetary resources which are multiplied by tradeoff constants. The expression for the general resource then becomes

$$V = \sum_{i=1}^m C_i + \sum_{j=1}^n k_j Q_j \quad (1)$$

where

C_i = monetary terms

Q_j = nonmonetary resources (measured in lb, watts, etc.)

k_j = tradeoff constant (\$/lb, etc.)

Lest the open-ended nature of the summation makes the problem appear intractable, let it be emphasized that for many feasibility studies the value equation involves only two or three terms.

The resources required for reliability improvement will be designated as V_r and those absorbed by cost of failure as V_f . In these symbols we can express a general criterion for economically justified reliability improvement as

$$\Delta V_r \leq -\Delta V_f \quad (2)$$

where it is understood that ΔV_f is the portion of the cost of failure eliminated by the reliability improvement costed as ΔV_r . Since the cost of failure will be reduced by the improvement, ΔV_f is a negative quantity, and the minus sign in relation (2) is required to permit comparison with the normally positive ΔV_r . Relation (2) is simply a mathematical restatement of the very first sentence of this section.

An alternative approach is to identify a total reliability sensitive cost applicable to a specified configuration (abbreviated in the following as "sensitive cost") as

$$V_t = V_r + V_f \quad (3)$$

where V_r is the reliability budget utilized in a configuration, and V_f represents the cost of failure for that configuration. In these terms, economically motivated reliability improvements will minimize total sensitive cost, and standard mathematical optimization techniques can be used to drive V_t to a minimum subject to invoked constraints. If we think of reliability

improvement as a step-wise process, the criterion for an economically justified step can be expressed as

$$V_{t2} \leq V_{t1} \quad (4)$$

where the subscript 1 refers to the condition prior to improvement and the subscript 2 refers to that following improvement. It is easily shown that condition (4) can only be satisfied if relation (2) holds.

In many situations the individual entries into the value equation (1) will not be known very accurately. The uncertainties can range from those associated with estimating the cost of a reliability improvement program to the much more fundamental ones of assigning a monetary equivalent for loss of satellite service or for restoration of confidence in a major system after a failure. However, the decision to proceed with a major computer reliability improvement often hinges on assigning a value to these intangibles, and it appears sound to do this deliberately rather than indirectly (e.g., by proceeding with a program based on benefits which have not been evaluated in economic terms). The prudent project manager will want to evaluate the desirability of a reliability improvement with both high and low estimates for expenditures and benefits, or use other methods of sensitivity analysis, before reaching the final decision.

In all specific examples treated below the expected value is used as a criterion for trading off costs and benefits of a reliability improvement. This implies that a 50 percent probability of a \$10,000 loss is treated as equal to a 1 percent probability of a \$500,000 loss. There will undoubtedly be some programs in which one of these conditions is much less acceptable than the other one. Where this is the case the general treatment presented here can still be followed; however, expected utilities of outcomes should be used instead of expected values (Ref. 2).

The criteria used here do not explicitly account for the point in time at which expenditures are made or losses may be incurred. Typically,

computer improvement costs must be paid in the near future whereas the cost of failure is incurred later. This is particularly significant when dealing with long-life satellites. Where an appreciable time period is expected to intervene between various expenditures used in the relations it will be desirable to convert all figures to a present-worth basis, standard techniques for which are described in most works on engineering economics (e.g., Ref. 3).

A number of specific problems that arise from the nature of spacecraft computers are: (1) inability to effect repair by direct access; (2) the critical dependence of the mission on continued operation of the computer and hence the large loss incident upon computer failure. These conditions require some special treatment of cost of failure computation for spacecraft computers. It has been convenient to investigate these for two distinct applications, the first of which is governed by mission reliability considerations, while the second one is governed by time-dependent reliability considerations. Cost of failure analysis for these two cases is presented in the following two sections.

SECTION 3

MISSION RELIABILITY MODEL

A typical application for the mission reliability model arises in the missile or booster area. Any substantial failure of a booster prior to payload separation will prevent attainment of mission objectives and will necessitate an additional launch. The loss that will be experienced is usually independent of the time of failure (as long as it occurs prior to payload separation). The cost of failure is zero if the booster survives, and it assumes a fixed value if a failure occurs. It is obvious that the key element in determining expected cost of failure is the probability of failure during the mission, or its complement, the mission reliability.

There are also a number of spacecraft applications to which the mission reliability model can reasonably be applied. Consider a spacecraft designed for investigation of seasonal variations of earth limb phenomena. By judicious selection of launch date and orbit, mapping of the seasonal phenomena can be accomplished in a single 90-day mission. However, each day of this mission supplies necessary information, and, if for some reason a failure should occur on the 60th day, the entire mission would have to be repeated with the proper calendric orientation. Thus, the loss due to a computer failure during the 90-day period is essentially independent of the time the failure occurs. This contrasts sharply with the cases considered in the following section.

The cost of failure calculations for cases to which the mission reliability model applies is quite simple. If mission reliability for the entire system is designated by R , the probability of mission failure is $F = 1 - R$. Cost of failure can be considered as a random variable, V_f , with the following assigned values:

$$\begin{aligned} V_f &= 0 && \text{if the mission succeeds} \\ &= L && \text{if there is a failure} \end{aligned}$$

The loss, L , will include the cost of a replacement launch and all associated factors discussed in the preceding section. For economic tradeoffs the expected value of the cost of failure will be used,

$$E[V_f] = F \cdot L \quad (5)$$

In optimizing computer reliability, we are concerned with the contribution that computer failure makes to overall mission failure. In the following, the mission reliability, R , is modeled by a two-block series arrangement of the computer, with reliability R_C , and all other spacecraft systems with reliability R_S . Thus,

$$R = R_C \cdot R_S \quad (6)$$

It is seen that

$$\frac{\partial R}{\partial R_C} = \frac{\partial F}{\partial F_C} = R_S \quad (7)$$

The incremental system failure reduction due to a computer improvement is given by

$$\Delta F = R_S \Delta F_C \quad (8)$$

The change in expected cost of failure due to computer improvement is found by combining Eqs. (5) and (8)

$$\Delta F[V_{fC}] = R_S \cdot L \cdot \Delta F_C \quad (9)$$

This equation can be used to evaluate the economic benefits for a proposed reliability improvement. In these circumstances the computer failure reduction, ΔF_C , and the associated resource expenditure, ΔV_r , will be

known. Multiplying the quotient of these quantities by $R_S L$ (constant for a given application) we form

$$-R_S L \Delta F_C / \Delta V_r = -\Delta E[V_{fC}] / \Delta V_r \quad (10)$$

Comparison of the right term with Eq. (2) shows that reliability improvement is economically justified as long as this fraction exceeds unity.

The cost of failure expression also permits identification of an optimum reliability level as follows. As discussed in Section 5, reliability improvements can be ordered to yield a concave plot such as that shown by curve V_r in Figure 1. The computer in which no specific expenditures for reliability improvement have been made is referred to as the baseline configuration. In this example, its failure probability is 0.20. The cost of a replacement launch in this figure is assumed to be \$20 million, and elements other than the direct replacement cost are assumed to increase the loss attendant upon a failure by 25 percent of the cost of a replacement launch, thus $L = \$25 \times 10^6$. The spacecraft system reliability, R_S , is taken as 0.8. Under these circumstances the expected cost of computer failure for the baseline configuration is \$4 million (obtained from Eq. (9) by using whole quantities instead of increments, permissible in a linear relationship). This cost will decrease linearly towards the origin as shown by the straight line $E[V_{fC}]$. It is seen that the sensitive cost, V_t , reaches a minimum when the computer failure probability is near 0.16. At this point, approximately \$350,000 has been allocated for reliability improvement with a corresponding decrease in failure probability of 0.04 below that achieved in the baseline configuration. Going beyond this point in reliability improvement, while reducing cost of failure, will not produce a decrease in sensitive cost and will thus not be economically justified by the criteria of Eq. (2) or (4). Again, let it be emphasized that in practical application of this technique a large amount of judgment is involved. In many cases the optimum will be defined as a range rather than as a point. The economic penalties due to this uncertainty are small.

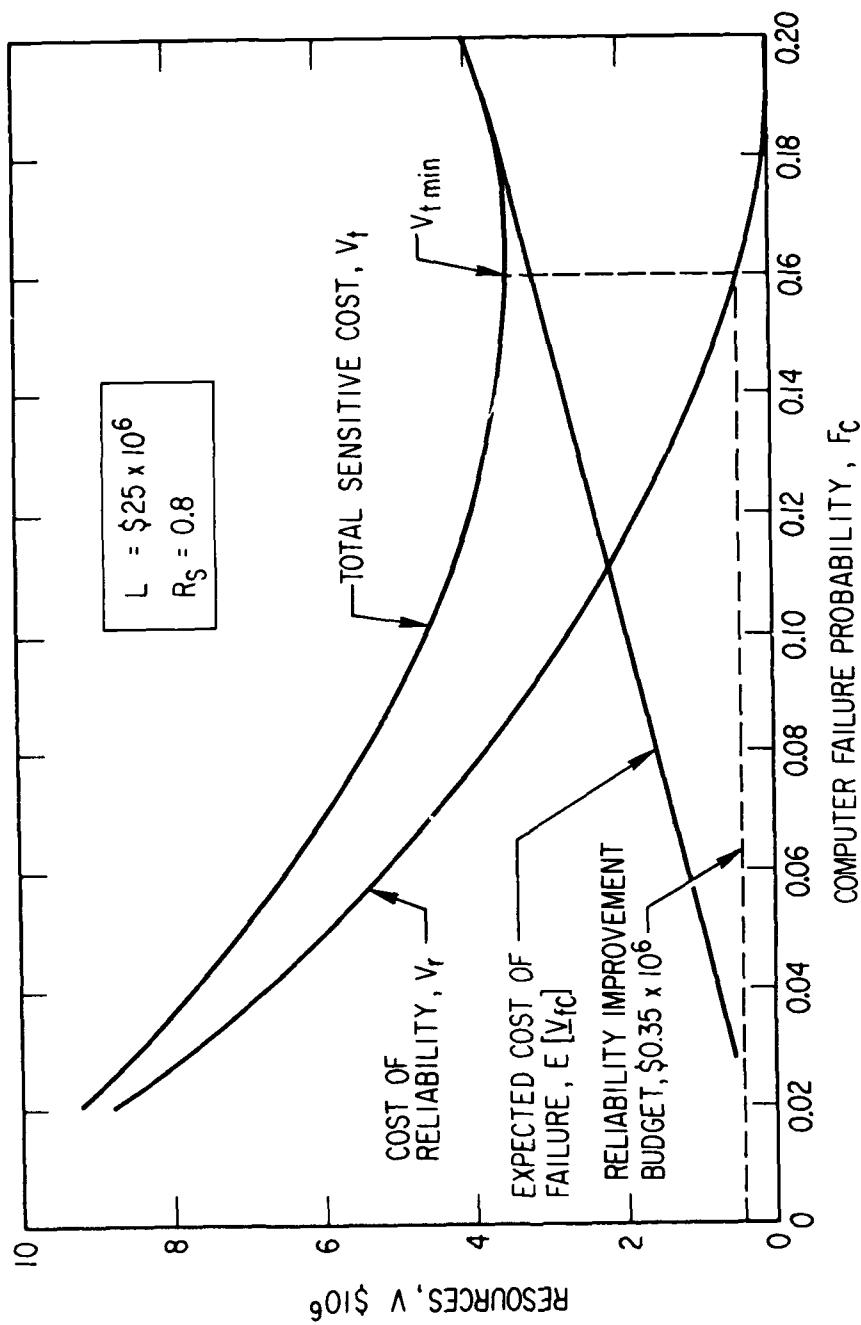


Figure 1. Mission Reliability Optimization, Low Cost Spacecraft

The same analysis applied to a spacecraft for which the cost of a replacement launch is \$50 million (all other factors remaining the same) is shown in Figure 2. Note the steeper slope of $E[V_{fC}]$ and movement of the minimum on the V_t curve to a failure probability of 0.10, at which point \$2.6 million are utilized for reliability improvement. This demonstrates that the application of a given computer to a more valuable spacecraft or mission requires higher expenditure for reliability improvement.

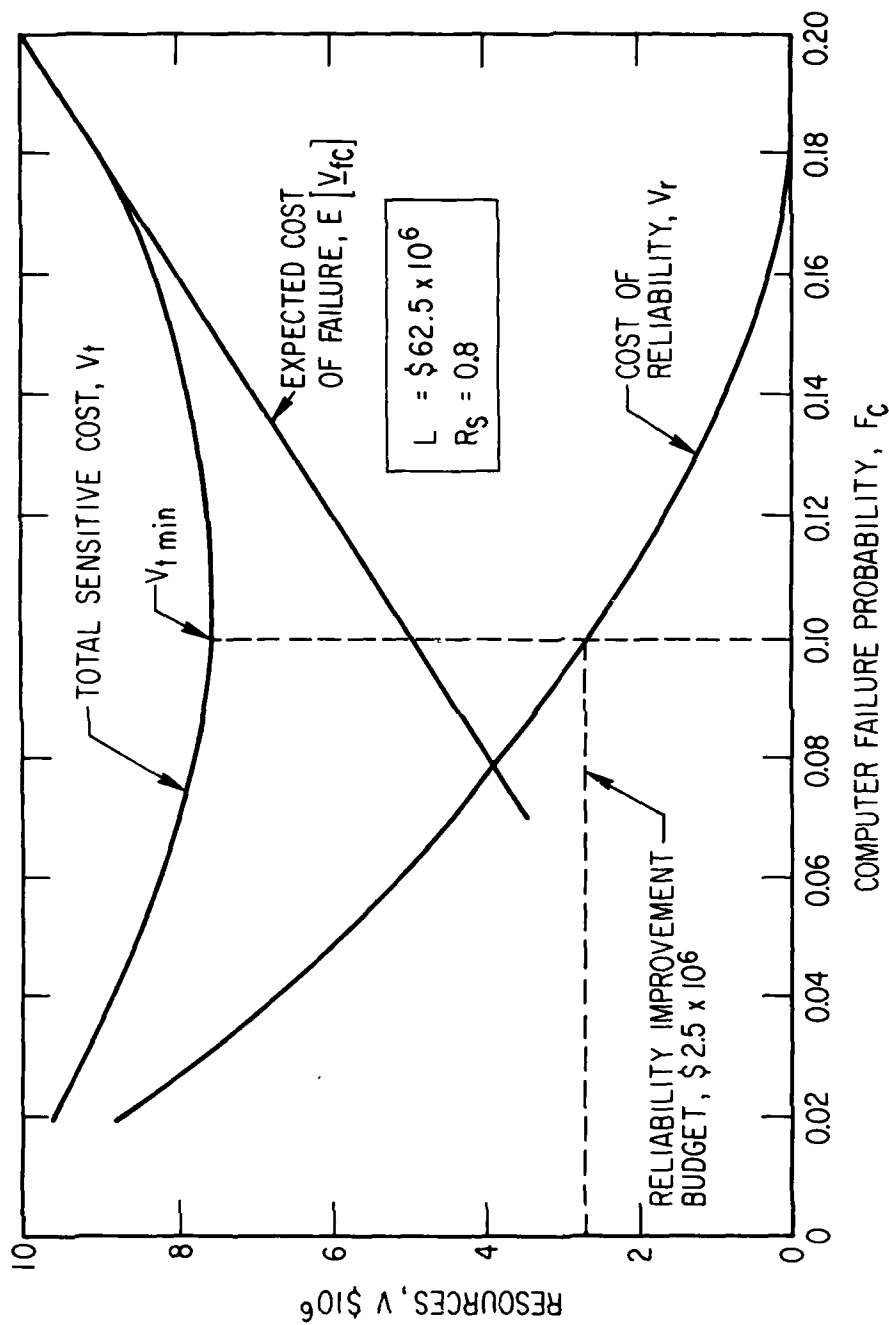


Figure 2. Mission Reliability Optimization, High Cost Spacecraft

SECTION 4

TIME-DEPENDENT RELIABILITY MODEL

The time-dependent reliability model is applicable to satellite missions requiring long life, including those with indefinite lifetime requirements. Communication, navigation, and meteorological satellites fall into this category. Although the individual satellite will have a limited lifetime (due to exhaustion of expendables, drag effects, etc.), referred to as the wear-out point, the mission requirement covers a long time span, extending in some cases over the entire foreseeable future. Thus, replacement launches are scheduled as a normal activity in the mission plan.

Loss of the satellite due to a computer failure near the wear-out point means that the time for replacement has been advanced only very little compared to the scheduled replacement. In contrast, damage occurring early means that the replacement satellite has to span almost the entire original satellite lifetime, and it will reach its own wear-out point close to the time when this was planned for the original one. Thus, cost of failure becomes dependent on the time of failure. It is high when failure occurs early in the satellite life, low if it occurs near the wear-out point.

This effect can be modeled by letting the loss become a function of the time of failure, t ,

$$\begin{aligned} L(t) &= L_0 (1 - t/W) & 0 \leq t \leq W \\ L(t) &= 0 & t > W \end{aligned} \tag{11}$$

where L_0 is computed in the same manner as the constant mission loss in the preceding section, and W is the wear-out life of the satellite. In this linear model, a failure occurring at the half-point of the wear-out life will then carry one-half of the loss that would be assessed against a failure during or right after launch. More elaborate modeling, including a range of wear-out times with an associated probability distribution may be desirable in some cases.

Also, the reliability of the other spacecraft systems decreases with time (reliability taken as the probability of not failing due to random events, distinct from wear-out which was discussed above). Repair of a satellite in orbit is not contemplated here, and therefore the spacecraft systems reliability, R_S , is a strictly decreasing time function. Eq. (9) shows that then a lower cost is assessed for late computer failure than for an early one. Typically, an exponential model for spacecraft reliability will be used such as

$$R_S(t) = e^{-st} \quad (12)$$

where s represents spacecraft hazard (the reciprocal of MTBF).

Another factor making cost of failure time-dependent is that advances in technology usually permit some performance or reliability improvement if the replacement is made late in the expected life of the original unit. Thus, late replacement permits desirable upgrading whereas early replacement does not. A closely related area is that performance requirements may change during expected lifetime of the satellite. Late replacement permits a more adequate response to the change in performance requirements.

Further, the cost of replacement, if it occurs early during the expected satellite life, translates into a higher "present worth" than if it occurs late. Another way of saying this is that interest is charged on the cost of the replacement from date of failure until the scheduled replacement date. For these latter factors, and particularly for the present worth, an exponential model may also be assumed. The exponents of these additional exponential factors can be combined with that of the reliability term, so that it is only necessary to make a numerical adjustment (increase) in s . In the following it is understood that s represents the total effect of all exponential terms.

For a given short period extending from t_1 to $t_1 + \Delta t$ it can be assumed that the loss and spacecraft reliability will be constant so that the cost of failure increment can be formulated as

$$E[V_{Cf}(\Delta t)] = L(t_1) R_S(t_1) F_C(\Delta t) \quad (13)$$

where $F_C(\Delta t)$ is the computer failure probability during Δt .

By letting the interval over which this expression is evaluated contract to the differential dt , we arrive at a form that can be integrated to yield the general time-dependent expected cost of failure for period T after launch

$$E[V_{fC}(T)] = \int_0^T L(t) R_S(t) \frac{dF_C}{dt} dt \quad (14)$$

It is further assumed that the computer reliability also follows the exponential model,

$$F_C(t) = 1 - e^{-ct} \quad (15)$$

where c is the hazard associated with the computer. From this, the failure density function for the computer is obtained as

$$\frac{dF_C(t)}{dt} = ce^{-ct} \quad (16)$$

Now, by substituting the specific model Eqs. (11), (12), and (16) into the general Eq. (14), and by making the limit of integration equal to the wear-out time, W , we obtain

$$\begin{aligned} E[V_{fC}(W)] &= cL_o \int_0^W (1 - t/W) e^{-(c+s)t} dt \\ &= \frac{cL_o}{c+s} \left[1 + \frac{e^{-W(c+s)} - 1}{W(c+s)} \right] \end{aligned} \quad (17)$$

To facilitate the application of this equation to practical problems it is convenient to introduce some nondimensional parameters. First, a normalized cost of failure is defined as

$$E[\underline{U}] \triangleq E[V_{fC}(W)]/L_o \quad (18)$$

Further, a normalized computer hazard

$$a = c/s \quad (19)$$

and a random failure factor

$$b = Ws \quad (20)$$

are introduced. For small values, b approximates the probability of a random spacecraft failure prior to wear-out. With these substitutions

$$E[\underline{U}] = \frac{a}{1+a} \left(1 + \frac{e^{-b(1+a)} - 1}{b(1+a)} \right) \quad (21)$$

This is seen to be a function of parameters a and b only. Solutions of Eq. (21) for a suitable range of these parameters are shown in Table 1.

As an example, consider a spacecraft MTBF of two years (this is an adjusted value to account for time-dependent factors other than reliability) and a wear-out life of one year. If the computer MTBF is four years ($a = 0.5$), then the normalized expected cost of failure due to the computer is 0.099. A reliability improvement that increases the computer MTBF to 6.7 years ($a = 0.3$) will bring the normalized cost of failure down to 0.061. If it costs less than the reduction in expected cost of failure, $0.038 L_o$, it is economically justified.

Selected results of Table 1 are graphically presented in Figure 3. A significant conclusion is that the expected cost of failure is a nearly linear

TABLE 1
NORMALIZED EXPECTED COST OF FAILURE
FOR THE TIME-DEPENDENT MODEL

a	b = 0.25	E[U]		
		0.5	1.0	2.0
0.1	0.011	0.021	0.036	0.054
0.2	0.023	0.041	0.070	0.103
0.3	0.034	0.061	0.101	0.149
0.5	0.055	0.099	0.161	0.228
0.7	0.076	0.134	0.213	0.295
1.0	0.107	0.184	0.284	0.377

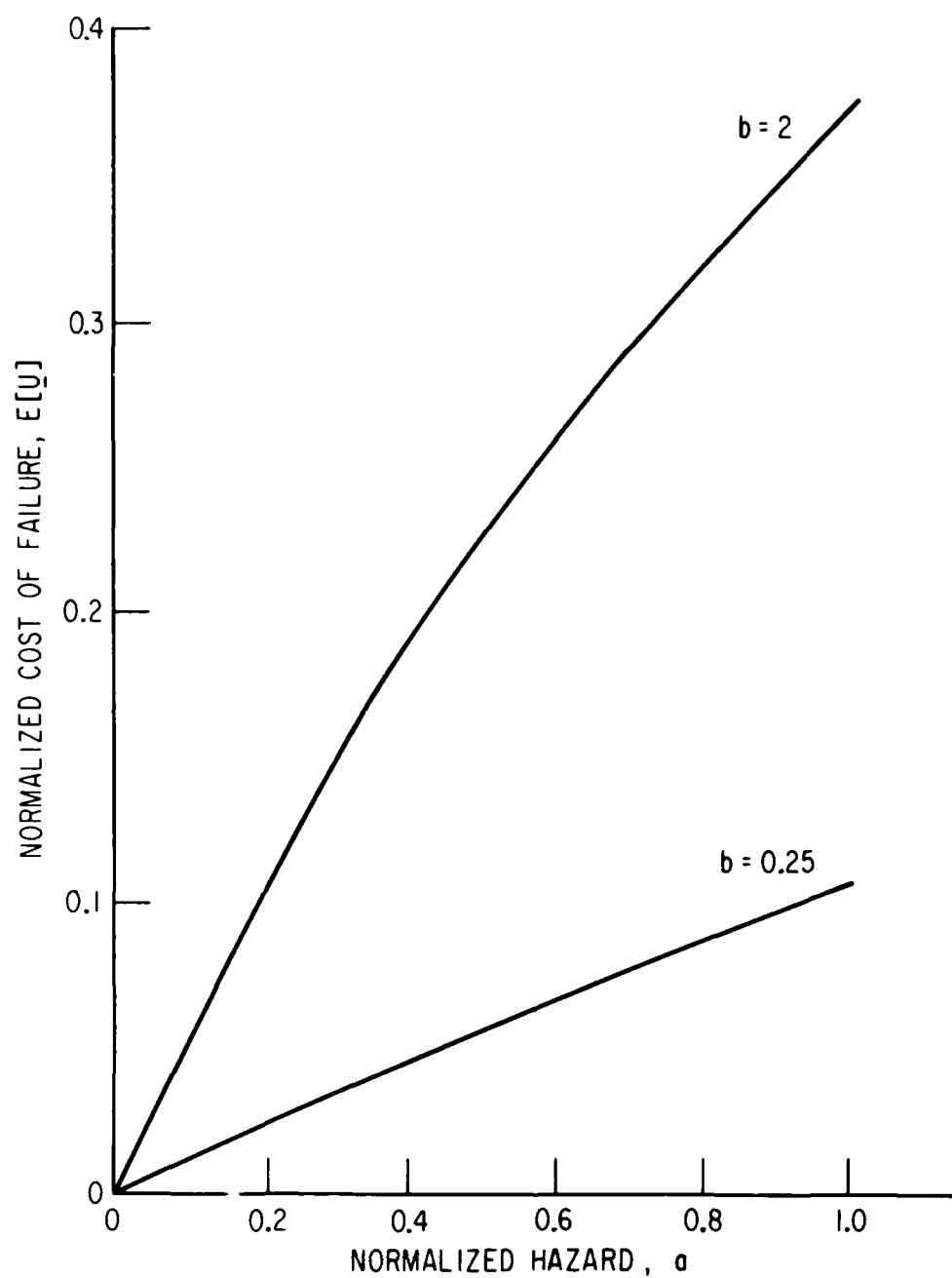


Figure 3. Expected Cost of Failure vs Computer Hazard

function of the nondimensional parameter, a . In the context of a specific decision on computer reliability improvement, the spacecraft hazard, s , can be assumed constant, and thus the expected cost of failure becomes a nearly linear function of computer hazard, c , only. This permits the optimization problem to be treated with the methods developed in the preceding section for the mission reliability model.

A specific example of reliability optimization for the time-dependent case is shown in Figure 4. The trend of the cost of reliability curve, V_r , is similar to that used in Figures 1 and 2, but note that the abscissa in Figure 4 represents computer hazard. The baseline spacecraft computer is assumed to have an MTBF of four years, thus $V_r = 0$ when $c = 0.25 \text{ year}^{-1}$. The loss, L_0 , is taken as $\$35 \times 10^6$, and for the parameters indicated in the figure the expected cost of failure for the baseline computer is $0.161 \times 35 \times 10^6 = \5.6×10^6 . This resource expenditure, plotted at the baseline computer hazard ($c = 0.25$), determines the key point of the $E[V_{fC}]$ line. All other steps in the procedure are identical to those used in the mission reliability case.

A number of gross simplifications have been utilized in this model. Wear-out has been assumed to occur at a definite point rather than over a period of time. The reliability functions of both the spacecraft and the computer have been assumed to be exponential. Other factors that tend to reduce the cost of failure with time have also been constrained to the exponential model and have been lumped with the reliability function. Improvement in these areas does not present particular difficulties from the mathematical point of view, but, in most cases, there will be insufficient data to provide suitable parameters for a more refined model equation. Additional research and documentation in these areas should be encouraged. In the meantime, the simplified model will be sufficient for many preliminary design purposes and should focus the attention on areas of critical data requirements.

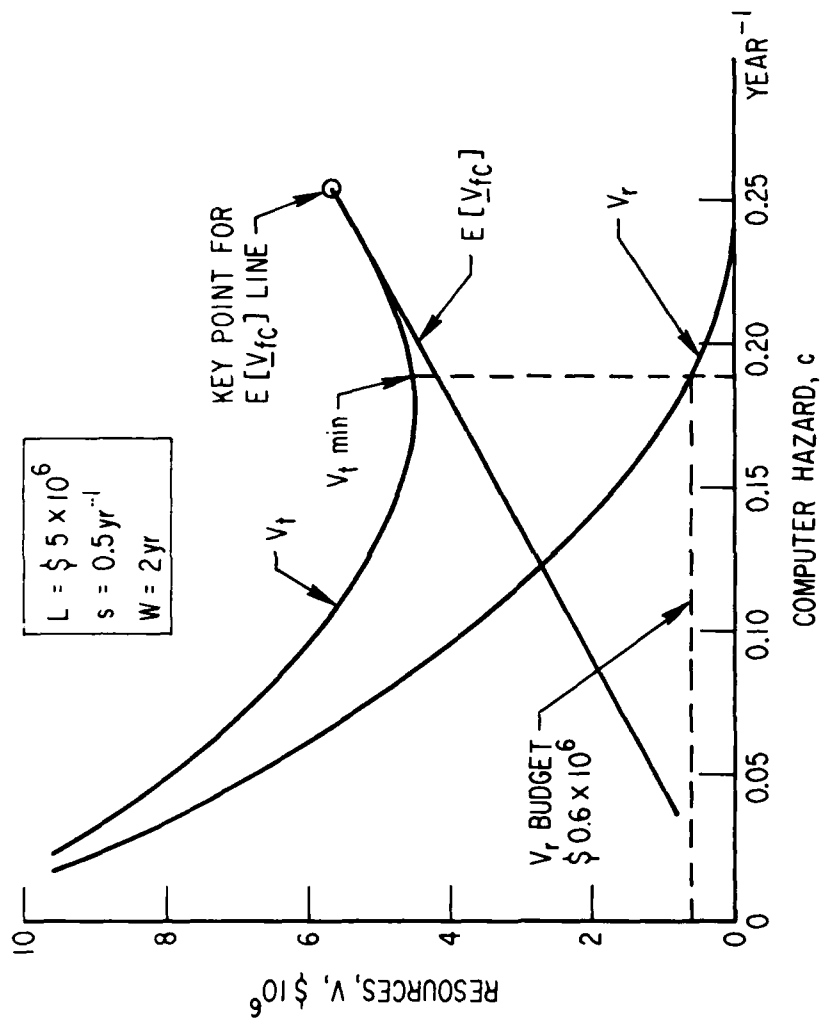


Figure 4. Reliability Optimization for Time-Dependent Case

SECTION 5

COST OF RELIABILITY IMPROVEMENT

In principle, the cost of reliability improvement, V_r , must be determined on a case-by-case method for each improvement under consideration. It is attempted here to furnish some guidelines on the formulation of individual estimates of V_r and for combining these into a plot of resource requirements versus reliability improvement as was utilized in previous figures.

It will be convenient to consider three basic types of reliability improvement:

- Massive or external redundancy
- Structured or internal redundancy
- Component improvement.

Massive redundancy implies installation of several complete computers with switchover or voting provisions to ensure continued flow of correct information after one or more computer failures. Massive redundancy can be effective for a wide spectrum of failures and therefore requires minimum a priori knowledge as to where failures occur and what causes them. Massive redundancy requires minimum modification of existing computer design and thus avoids development risk. On the other hand, it involves considerable expenditure in resources for reliability improvement.

Structured redundancy involves redundancy within the computer itself (e.g., by duplicating registers or memory arrays so that the probability of failure of a given computer is reduced). Proper implementation of structured redundancy requires knowledge of the distribution of failures by computer function so that the elements that contribute most to failure can be made redundant. Emphasis is on knowing the manifestation of failure rather than the cause. Since the computer structure is being modified, structured redundancy involves some development risk. On the other hand, expenditure of a given amount of resources usually provides a higher degree of reliability improvement by structured redundancy than could be achieved in massive redundancy.

One of the reasons is that structured redundancy can attack the areas of the computer where the highest concentration of failures is found. Another reason is that structured redundancy can take advantage of redundancy for multiple elements. If eight similar registers are employed in a computer, each one being 0.99 reliable, the entire structure is only 0.92 reliable which may not be sufficient. However, by providing a single spare register with capability of switching it for a faulty unit, the overall probability of failure can be brought up to approximately 0.99, almost as high as if the complete register structure were duplicated. Even when due allowance is made for the cost of failure detection and switching (and for the imperfections in these) the redundancy for multiple elements is a very attractive reliability tool.

Component improvement is here taken to comprise improvement in both the manufacturing and testing, the latter sometimes being considered as a separate improvement method (screening). To implement a successful component improvement program the parts responsible for a high percentage of failures as well as the failure mechanism must be known. Even with this knowledge the success of the improvement, and the interaction of the improved component with the computer system, cannot be assured. Thus, component improvement carries a high development risk. Where it is applicable and successful, it provides reliability improvement at a rather low resource expenditure (e.g., where bond failures are a problem it is obviously cheaper to improve bonding than to duplicate shift registers or entire computers).

The ranking of reliability improvements cannot proceed blindly on the basis of failures removed per unit resource. The risk associated with each of the improvements must also be weighed. There are risks that the anticipated improvement will not be achieved by the time required, that the estimated resource expenditure will be exceeded, and that unanticipated interactions with the rest of the system are encountered. It is in the following assumed that some decision regarding the acceptable risk has been taken and that feasible improvements that are acceptable by this criterion have been identified.

An example evaluation of two hypothetical improvements that carry acceptable risk is shown in Table 2. The baseline computer cost, C_o , is \$500,000, weight, W_o , is 50 lb, and mission reliability, R_o , is 0.85. Resource expenditures for power and environmental factors are considered negligible. The improvements under consideration are simple redundancy and triple modular redundancy (TMR), both implementations of massive redundancy.

In simple redundancy, another computer is installed and processes the identical input. There is a direct hardware addition for the second computer, and an indirect one (assumed equivalent to one-fifth of a computer) for a switching module. There are also software costs for comparison and synchronization. Prior to issuance of a significant output (e.g., steering command) a comparison is made. If there is agreement, the command is issued. If there is no agreement, each computer goes into a diagnostic routine. If one of these fails, the output of the other computer is sent as a command. If none fails, one of the outputs is selected at random. The diagnostic routine is assumed to provide 60 percent coverage and random selection is assumed to be 50 percent correct in the remaining cases. Thus, 80 percent of the decisions will be correct if at least one computer operates. The probability that both computers operate is $0.85^2 = 0.73$, and the probability that both fail is 0.02. Therefore, the probability of one computer operating is 0.25. The 80 percent probability of correct decision is applied to this number to yield a total improvement 0.20. This is added to the original 0.73 probability of success to yield the new mission reliability of 0.93.

The TMR configuration requires the addition of two computers and a voting network, the latter assumed equal to one-half computer. Software costs are assumed identical with those for simple redundancy. The intrinsic reliability for the TMR system, obtained from Ref. 4, is 0.94. In the remaining 6 percent, random selection will be used and is assumed to be correct in one-half of these cases. This yields a total mission reliability of 0.97.

TABLE 2
EVALUATION OF IMPROVEMENT
BY MASSIVE REDUNDANCY

	<u>Simple Redundancy</u>	<u>TMR</u>
Direct Hardware Addition	1	2
Indirect Hardware Addition	0.2	0.5
Total Hardware Addition, q_1	1.2	2.5
Cost of Hardware Addition, Addition, $C_1 = q_1 C_o$, \$	0.6×10^6	1.25×10^6
Cost of Software Addition, C_2 , \$	0.5×10^6	0.5×10^6
Weight Addition, $Q_1 = q_1 W_o$, lb	60	125
Weight Tradeoff Factor, k_1 \$/lb	10,000	10,000
Total Resource Addition, $V_r = C_1 + C_2 + k_1 Q_1$, \$	1.7×10^6	3×10^6
Mission Reliability, R_C	0.93	0.97
Improvement per Unit Resource, $-\Delta F_C / \Delta V_r$ (\$ ⁻¹)	0.047×10^{-6}	0.040×10^{-6}

The results of these calculations are plotted in Figure 5a. The individual points correspond to the failure probability and resource expenditures from Table 2. However, the slope of the line connecting the TMR and simple redundancy coordinates represents the selection criterion referred to in Eq. (10). For this segment, $-\Delta F_C = 0.04$ and $\Delta V_r = \$1.3 \times 10^6$, these numbers represent the difference between the two improvements in Table 2. In this example, $-\Delta V_r / \Delta F_C$ for the increment is $\$32.5 \times 10^6$. If the product, R_{SL} , exceeds this amount, TMR is preferred over simple redundancy by economic criteria (Eq. (10)). Equivalent calculations can be performed for the time-dependent case.

The general aim of the procedure is to produce a ranking of failure improvement per unit resource expenditure for all improvement proposals carrying an acceptable risk. Where detailed data on specific improvements are available (which may at times be dependent on one another), a number of analytical and computer-programmed techniques can be used for producing a suitable ordering (Refs. 5 and 6). Where data on specific improvements are not available but where the distribution of failures among elements of the computer (and the cost of the elements) is known, the failure/value ratio technique can be used to identify the most profitable improvements (Ref. 7).

By these techniques a concave polygon such as the one shown in Figure 5b can be constructed. In accordance with the remarks earlier in this section it will be generally found that the major reliability improvement methods are grouped as indicated in this figure. The polygon or some other curve fitted through a number of points can then form the basis for defining an optimum reliability level as discussed in Section 3.

In practice, the cost of reliability improvement will be evaluated repeatedly, starting with the conceptual phase of the mission, when overall reliability requirements are established, and continuing through the qualification test of the computer, when final decisions about replacement of questionable parts or processes may be made. The estimates for the cost of improvement will obviously be better in the later phases of the program. It must be recognized, however, that important decisions about the overall computer

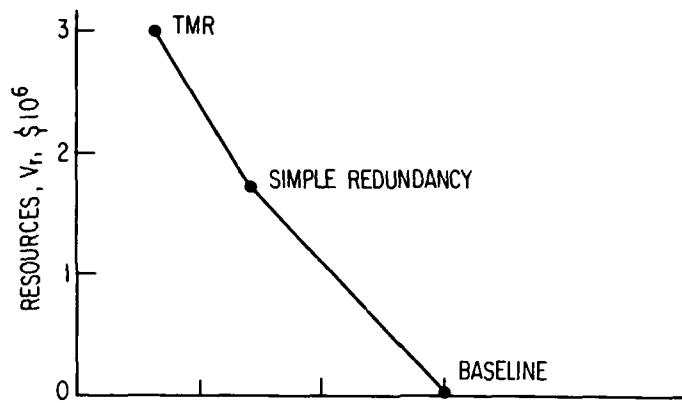


Figure 5a. Cost of Reliability Improvement
Improvements due to Massive Redundancy

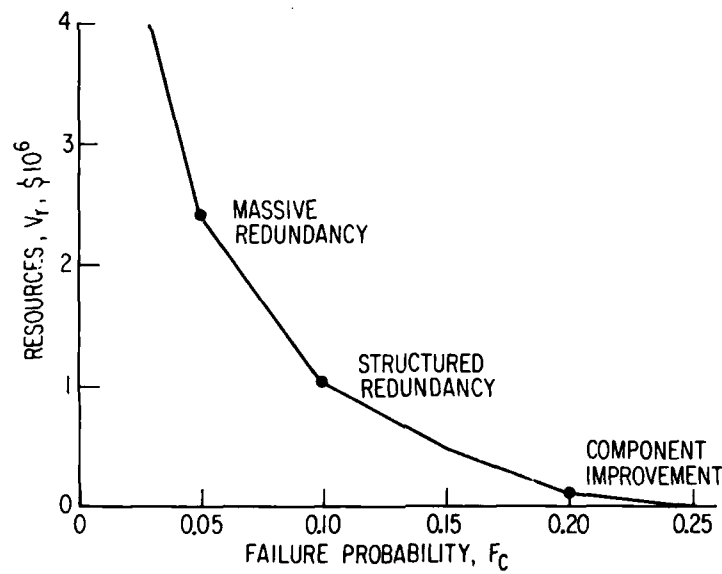


Figure 5b. Cost of Reliability Improvement
General Trend

configuration are made early, when only partial information may be available. Some of the approximations used in the previous sections and discussion of trends presented here may be particularly useful in these early phases.

SECTION 6

CONCLUSIONS

The field of spacecraft digital computers is still in its infancy. For effective use, a computer has to interface with many spacecraft systems, and it becomes a major series element for mission accomplishment. Thus, the entire mission may then be jeopardized by a computer failure. Under these circumstances there is much concern with computer reliability, and it has here been attempted to develop guidelines for an economically optimum level of reliability improvement.

The general strategy is to proceed with each step in the improvement only if the expected reduction in cost of failure exceeds the cost of the improvement. To this end, techniques for calculating cost of failure have been described, and, in particular, a new technique for evaluating cost of failure for long-time spacecraft missions has been developed.

After an optimum level of reliability has been specified, the designer has several options of proceeding with improvement of the basic computer structure: massive redundancy, structured redundancy, and component improvement. There are general trends among these with regard to cost per failure removed and with regard to the development risk. Guidelines for assessment of the economic impact of various improvement techniques have been presented.

Economic evaluation of reliability requirements and techniques is at present not an exact science. A number of procedures have been developed here as an aid in making the process more objective. Where possible, mathematical models have been used for ease of analysis and communication. These are intended to supplement, by no means to replace, good judgment which is essential for program management, design, and application of spacecraft computers.

REFERENCES

1. Digest, 1971 International Symposium on Fault-Tolerant Computing, IEEE Computer Society, 1-3 March 1971, Pasadena, California.
2. Hall, Arthur D., A Methodology for Systems Engineering, D. Van Nostrand, Princeton, N. J., 1962, Chapters 10 and 11.
3. Barish, Norman N., Economic Analysis, McGraw-Hill Book Company, New York, 1962, Section 10.
4. Mathur, Francis P., "Reliability Modeling and Analysis of a Dynamic TMR System Utilizing Standby Spares", 7th Annual Allerton Conference on Circuits and Systems, October 1969.
5. Neuner, G. E., and R. N. Miller, "Resource Allocation for Maximum Reliability", Proceedings of the 1966 Annual Symposium on Reliability, IEEE Cat. No. 7 C 26, pp. 322-346, 1966.
6. Barlow, Richard E., and Frank Proschan, Mathematical Theory of Reliability, John Wiley & Sons, New York, 1965.
7. Hecht, H., "Economics of Reliability Improvement for Space Launch Vehicles", Aerospace Report No. TR-0158(9990)-1, June 1968. (Essentially identical with dissertation, UCLA, 1967)